UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF OHIO
EASTERN DIVISION

UNITED STATES OF AMERICA,	)	**CASE NO. 1:18CR561**
	)	
Plaintiff,	)	**JUDGE CHRISTOPHER A. BOYKO**
	)	
vs.	)	
	)	
JACOB L. MACLIN,	)	**OPINION & ORDER**
	)	
Defendant.	)	

CHRISTOPHER A. BOYKO, J.:

Defendant Jacob Maclin asks this Court to suppress evidence found at his residence, in a Dropbox account and to suppress certain statements he made to authorities. (Doc. 10). Because investigators did not violate either of Defendant's Fourth or Fifth Amendment rights, the Court **DENIES** Defendant's Motion without a hearing.

I. BACKGROUND FACTS

Onset of the Investigation

In December of 2017, Homeland Security Investigators ("HSI") in Pittsburgh, Pennsylvania arrested an individual by the name of "Dubois." HSI arrested Dubois for Traveling to Meet a Minor. A subsequent investigation into Dubois revealed he engaged in various chats on KIK Messenger ("KIK").[1] One such conversation involved the user

[1] "KIK Messenger, commonly called KIK, is a proprietary instant messenger software application (app) for mobile devices. It uses a smartphone's data plan or Wi-Fi to transmit and receive messages, photos, videos, sketches, mobile webpages, and other content...KIK is known for its features preserving users' anonymity, such as allowing users to register without providing a telephone number, and preventing users from being located on the service (including by the company itself) through any information other than their chosen username." (Doc. 12-1, ¶ 8).

"curiousdude4321." Dubois's KIK chat history also reflected a shared access to a Dropbox[2] account associated with the email address "jake.sawyer239@yahoo.com".

On December 26, 2017, investigators sent a formal request to Dropbox, Inc. to preserve all records and files relating to the jake.sawyer239@yahoo.com account. Pittsburgh HSI also issued a summons to Dropbox, Inc. for account and IP log information related to the same account. The information Dropbox provided in response included a single account login from IP address 108.66.122.200 on January 1, 2018. Additionally, the response provided a User ID ending in 8145.

Investigators also sent a summons to KIK regarding the subscriber information for curiousdude4321. KIK responded on January 5, 2018 with the information, including IP login information for the account from December 7, 2017 through January 1, 2018. Sixty out of sixty-five logins utilized IP address 108.66.122.200, the same IP address that logged into the jake.sawyer239@yahoo.com Dropbox account. This IP address was assigned to an AT&T U-Verse customer in northeastern Ohio. The remaining IP addresses were assigned to Verizon Wireless.

Cleveland Investigation

On January 11, 2018, HSI Pittsburgh referred the investigation to the HSI Cleveland office. On January 23, 2018, Cleveland investigators issued two summonses. The first they sent

[2] "Dropbox is a file hosting service operated by Dropbox, Inc...that offers cloud storage, file synchronization, personal cloud, and client software. Dropbox...allows users to create a special folder on each of their computers, which Dropbox...then synchronizes so that it appears to be the same folder (with the same contents) regardless of which computer is used to view it. Files placed in this folder also are accessible through a website and mobile phone applications." (Doc. 12-1, ¶ 12, n.1).

to AT&T for user information related to the IP address 108.66.122.200, the IP address used to access both KIK and Dropbox. AT&T responded on January 30, 2018, indicating that the customer was Langston Maclin with an address of XXXX Baintree Road, University Heights, Ohio 44118. Public records confirmed Mr. Maclin owns the Baintree residence.

The second summons investigators sent was to Verizon Wireless for the other five IP addresses used to access the KIK account. The only common phone number to access the different IP addresses during the relevant times was (216) 906-****. This phone number was associated with an account in the name of Mr. Maclin.

A review of public records indicated that Defendant, Mr. Maclin's son, also resided at the Baintree residence. Investigators compared KIK communications, state records and Facebook information to confirm curiousdude4321 was likely Defendant. They based this determination on the fact that curiousdude4321 claimed his age to be 23, the same as Defendant. It is also based on images posted on KIK that resemble Defendant's Facebook pictures.

Search of Baintree Residence

Based on the above, Special Agent Michael Deterling applied for a Search Warrant of the Baintree residence. Magistrate Judge David Ruiz granted the Search Warrant on April 13, 2018. On April 17, 2018, law enforcement from three different agencies executed the Search Warrant. Authorities found Defendant home alone. They removed Defendant and took him to a mobile forensic lab parked in front of the residence for an interview. Investigators informed Defendant he was not under arrest, he did not have to answer any questions and he could leave at any time. Despite these options, Defendant chose to stay and answer questions. During the interview, Defendant admitted to using KIK and viewing child pornography.

Search of jake.sawyer239@yahoo.com Dropbox Account

On April 13, 2018, Agent Deterling applied for a Search Warrant to review the contents of the jake.sawyer239@yahoo.com account. Specifically, Agent Deterling stated "[t]he property to be searched is the Dropbox ***user account(s) and content*** associated with the following email address: jake.sawyer239@yahoo.com." (emphasis added). The Magistrate Judge granted the Search Warrant.

On April 30, 2018 Dropbox responded. Dropbox provided information related to a User Account ending in 7676. There was no content associated with this account. Agent Deterling noticed an error in Dropbox's production as the account provided did not correspond with the information previously preserved and supplied to Pittsburgh HSI. Deterling followed up with Dropbox and requested information associated with Dropbox User Account ending 8145.

On May 2, 2018, Dropbox responded. Dropbox indicated the Deterling was correct and that two separate User Accounts were registered to jake.sawyer239@yahoo.com. Dropbox provided content associated with User Account 8145 the next day. An analysis indicated that the account contained approximately 1136 images and 79 video files showing the sexual exploitation of minors.

On September 26, 2018, the Grand Jury indicted Defendant with one count of Receipt and Distribution of Visual Depictions of Real Minors Engaged in Sexually Explicit Conduct, in violation of 18 U.S.C. § 2252(a)(2); and one count of Possession of Child Pornography, in violation of 18 U.S.C. § 2252A(a)(5)(B). Defendant moved to suppress the evidence recovered from his residence, from Dropbox and his statements made to authorities on February 26, 2019. (Doc. 10). The Government opposed on March 12, 2019. (Doc. 12).

II. LAW & ANALYSIS

A. Standard of Review

The Fourth Amendment to the United States Constitution states:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violation, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. CONST. amend. IV.

Probable cause is defined as "reasonable grounds for belief, supported by less than prima facie proof, but more than mere suspicion" and exists "when there is a 'fair probability' given the totality of the circumstances, that contraband or evidence of a crime will be found in a particular place." *United States v. Lattner*, 385 F.3d 947, 951 (6th Cir. 2004), *cert. denied*, 543 U.S. 1095 (2005) (citing *United States v. Davidson*, 936 F.2d 856, 859 (6th Cir. 1991)).

In *Illinois v. Gates*, the Supreme Court announced the basic standard for determining whether an affidavit establishes probable cause to issue a search warrant:

> The task of the issuing magistrate is simply to make a practical, commonsense decision whether, ***given all the circumstances set forth in the affidavit*** before him [or her], ... there is a fair probability that contraband or evidence of a crime will be found in a particular place. And the duty of the reviewing court is simply to ensure that the magistrate had a substantial basis for concluding that probable cause existed.

426 U.S. 213, 238-39 (1983) (emphasis added); *see also United States v. Helton*, 314 F.3d 812, 819 (6th Cir. 2003); *Davidson*, 936 F.2d at 859.

A finding of probable cause "should be paid great deference by reviewing courts." *Gates*, 462 U.S. at 236. However, reviewing courts must ensure that the issuing magistrate or judicial officer did "not serve merely as a rubber stamp for the police." *United States v. Leon*,

468 U.S. 897, 914 (1984) (quoting *Aguilar v. Texas*, 378 U.S. 108, 111 (1964)). Further, reviewing courts "will not defer to a warrant based on an affidavit that does not 'provide the magistrate with a substantial basis for determining the existence of probable cause.'" *Id.* at 915 (quoting *Gates*, 462 U.S. at 239).

Defendant argues the Search Warrants issued for his residence and Dropbox violated the Fourth Amendment. The crux of his argument is that investigators gathered evidence from online service providers without warrants. Accordingly, investigators could not rely on that information to support the Search Warrants.

B. Warrantless Searches

Defendant claims law-enforcement failed to obtain a warrant on two separate occasions. The first when authorities relied solely on administrative summonses. And the second when investigators searched the jake.sawyer239@yahoo.com account a second time without a warrant. For the following reasons, Defendant's claims have no merit.

i. Administrative Summonses

Investigators used administrative summonses to obtain a variety of information throughout their investigation. Defendant claims the use of these summonses violated his Fourth Amendment rights. Particularly, Defendant relies on *Carpenter v. United States,* 138 S. Ct. 2206 (2018) to argue that, like the "cell-site location information" or "CSLI" in *Carpenter,* the Government must obtain a warrant prior to receiving subscriber information from internet providers. The Government disagrees and claims *Carpenter* is distinguishable due to the differences between CSLI and subscriber information.

Typically, "a person has no legitimate expectation of privacy in information...voluntarily

turn[ed] over to third parties." *Carpenter*, 138 S.Ct. at 2216. This is true "even if the information is revealed on the assumption that it will be used only for a limited purpose." *Id.* This 'third-party doctrine' has limits however, as "the Supreme Court declined to extend the rule to [*Carpenter*'s] cell-site records that convey 'a detailed and comprehensive record of [a] person's movements.'" *United States v. Contreras*, 905 F.3d 853, 857 (5th Cir. 2018) (quoting *Carpenter*, 138 S.Ct. at 2217). Despite *Carpenter*'s limitation, "the third-party doctrine continues to apply to 'business records that might incidentally reveal location information,' including telephone numbers and bank records." *Id.* (quoting *Carpenter*, 138 S.Ct. at 2220). Accordingly, the government may compel the disclosure of certain basic information maintained by providers of computing services via administrative subpoenas. 28 U.S.C. § 2703(c).

Investigators in *Carpenter* relied on § 2703 to obtain cell phone records for a suspect. *Carpenter*, 138 S. Ct. at 2212. The information investigators received contained CSLI, which is data collected by wireless carriers to aid certain business purpose. *Id.* at 2211-12. CSLI can also provide precise location information depending on the size of the geographic area covered by the cell site. *Id.* at 2211. Due to the ever-increasing use of cell phones, the precise location of the average user throughout a fixed period is readily obtainable. *Id.* at 2211-12. Investigators in *Carpenter* utilized over 127 days of CSLI data to determine Carpenter was "right where the...robbery was at the exact time." *Id.* at 2213.

In a "narrow decision" and given the "unique nature" of CSLI, the Supreme Court held "an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI." *Id.* at 2217. Accordingly, when investigators wish to acquire a suspects location by use of CSLI, they must "obtain a warrant...before acquiring such

records." *Id.* at 2221.

Upon review, the Court agrees with the Government. The subscriber information investigators obtained here is different than the CSLI obtained in *Carpenter*. CSLI provides the precise location of Defendant; subscriber information does not. Rather, investigators must take separate actions to make that information valuable. Moreover, CSLI follows the phone carrier around just by virtue of activating the cell phone. Subscriber information requires an individual's active participation – the subscriber only captures information when the platform is used. Thus, authorities are unable to determine a suspect's precise location or his daily movements by virtue of subscriber information alone.

This determination is in line with other courts that have addressed the issue post-*Carpenter*. *See United States v. Hood*, 920 F.3d 87, 92 (1st Cir. 2019) (Defendant did not have a reasonable expectation of privacy in the information that the government acquired from KIK without a warrant); *Contreras*, 905 F.3d at 857 (5th Cir. 2018) (IP address information "falls comfortably within the scope of the third-party doctrine. [The provider's] records revealed only that the IP address was associated with the Defendant's residence. They had no bearing on any person's day-to-day movement"). Accordingly, the investigators use of summonses to KIK, Dropbox, AT&T and Verizon Wireless were proper.

ii. Search of Dropbox Contents

When responding to the Search Warrant, Dropbox provided information relating to User Account ending in 7676. This User Account did not coincide with information previously preserved. Therefore, agents requesting Dropbox provide information pertaining to User Account ending in 8145. Dropbox complied.

Defendant mistakenly claims agents should have obtained a second warrant before they could request information about User Account 8145. In doing so, Defendant overlooks the actual language of the Search Warrant: the Magistrate Judge authorized agents to search "the Dropbox user account(s) and content associated with" jake.sawyer239@yahoo.com. Thus, not only was Dropbox's initial response incomplete, the Search Warrant authorized agents to search "user account(s)" of jake.sawyer239@yahoo.com.

Since the Search Warrant authorized investigators to search multiple user accounts, the Court finds no problem with agents ensuring compliance with its terms.

C. Search Warrant for Residence

Defendant first challenges the Affidavit for Search of the residence because it encompasses information obtained without a warrant. As determined above however, this argument is without merit. Agent Deterling therefore properly utilized the information in his Affidavit for Search.

Further, the Court disagrees with Defendant's other arguments that the Affidavit for Search, even if it included all information, failed to establish probable cause. Defendant relies on *United States v. Falso*, 544 F.3d 110 (2d Cir. 2008) to support his argument. In *Falso*, the Second Circuit reversed the district court and determined the search warrant did not establish a substantial basis for probable cause. *Falso*, 544 F.3d at 124. The court reached this conclusion on two bases. First, the affidavit did not contain allegations that the defendant in fact gained access to the website alleged to contain child pornography. *Id.* Second, because the affidavit did not contain any allegations to support the inference that the website's sole purpose was the viewing and sharing of child pornography. *Id.*

Unlike *Falso* however, the Affidavit alleges Defendant actually accessed the Dropbox account thought to contain child pornography. The same IP address used for KIK logged into the Dropbox account. Further, the Affidavit relays pages of conversation where the participants discuss and share child pornography. The Affidavit contains allegations of curiousdude4321 (believed to be Defendant) actually sharing images of child pornography. Thus, there are ample examples of Defendant's active participation in soliciting and sharing child pornography as compared to the defendant in *Falso*. Accordingly, Defendant's reliance on *Falso* is misplaced.

Defendant also makes a staleness argument: the excerpted communications discussing child pornography from KIK occurred before the confirmed logins from Defendant's IP address. Thus, there was no proof that Defendant utilized KIK to transact in child pornography. While not specifically referred to as such, Defendant seems to imply the KIK conversation is stale evidence that cannot be used to support a probable cause determination.

"[I]n seeking to establish probable cause to obtain a search warrant, the affidavit may not employ 'stale' information, and whether information is stale depends on the 'inherent nature of the crime.'" *United States v. Brooks*, 594 F.3d 488, 493 (6th Cir. 2010). In analyzing whether information is stale, the Sixth Circuit considers the following factors: "the character of the crime (chance encounter in the night or regenerating conspiracy?); the criminal (nomadic or entrenched?); (3) the thing to be seized (perishable and easily transferrable or of enduring utility to its holder?); [and] the place to be searched (mere criminal forum of convenience or secure operational base?)." *United States v. Spikes*, 158 F.3d 913, 923 (6th Cir. 1998). Given the nature of child pornography, courts in the Sixth Circuit have routinely found that evidence in support of child pornography does not often go stale. *See United States v. Hampton*, 504 Fed.

App'x 402, *2 (6th Cir. Nov. 5, 2012) (collecting cases with respect to stale evidence and child pornography).

Likewise, the KIK communications are not stale. All four of the above factors support this conclusion. First, "child pornography is not a fleeting crime." *United States v. Frechette*, 583 F.3d 374, 378 (6th Cir. 2009). The crime is "generally carried out in the secrecy of the home and over a long period." *Id.* (quoting *United States v. Paull*, 551 F.3d 516, 522 (6th Cir. 2009)). Second, Defendant was not nomadic. The allegations in the Affidavit alleged that sixty of the sixty-five KIK logins were from his residential address. Third, investigators sought to seize electronics and cell phones for images of child pornography. As courts have previously determined, "images of child pornography can have an infinite life span." *Id.* (citing *United States v. Terry*, 522 F.3d 645, 650 n.2 (6th Cir. 2008)). Finally, investigators wished to search Defendant's residence, "which is clearly a 'secure operational base.'" *Id.* (quoting *Paull*, 551 F.3d at 522). Accordingly, the *Spikes* factors indicate that the KIK communications were not stale in this case.

Finally, Defendant believes investigators needed to confirm that the Dropbox account contained child pornography. This belief is unreasonable. During the KIK conversations, participants openly discussed images of child pornography. Curiousdude4321 stated his images were contained on Dropbox. When Dubois obtained the Dropbox login information, he checked with curiousdude4321 to confirm the information. Curiousdude4321 confirmed, supporting it was the same account where his images of child pornography were stored.

Accordingly, the Affidavit for Search of Defendant's residence contained ample evidence to give the Magistrate Judge a substantial basis to determine that evidence of illegal

advertisement, distribution, receipt and possession of child pornography would be found at Defendant's residence.

D. Search Warrant for Dropbox

Defendant also asserts that the Affidavit for Search of Dropbox was not supported by probable cause. Before doing so however, Defendant must demonstrate that he has an expectation of privacy in the Dropbox account. Since Defendant has not done so, his Fourth Amendment challenge fails.

Before a defendant can claim his Fourth Amendment rights were violated, he must demonstrate he had "an expectation of privacy in the place searched" and that "his expectation was reasonable." *Minnesota v. Carter*, 525 U.S. 83, (1998); *see also United States v. Pollard*, 215 F.3d 643, 647 (6th Cir. 2000). "A defendant must satisfy a two-pronged test to show a legitimate expectation of privacy: 1) he must manifest an actual, subjective expectation of privacy; and 2) that expectation is one that society is prepared to recognize as legitimate." *Pollard*, 215 F.3d at 647 (citation omitted).

Defendant makes no argument that he has a subjective expectation of privacy in the jake.sawyer239@yahoo.com Dropbox account. Rather, he tries to distance himself from any association with the account. He argues the Affidavit does not contain evidence that he owned or otherwise accessed the account. And while he admits to having a Dropbox account, he argues there is no proof that it is the jake.sawyer239@yahoo.com account.

The Fourth Amendment protects people, not places. *Katz v. United States*, 389 U.S. 347, 351 (1967). Yet Defendant asks the Court to protect a place – the Dropbox account – against unreasonable searches with no regard to Defendant's privacy interest to the account. This lack

of subjective privacy interest in the Dropbox account is fatal to Defendant's claim.

Moreover, even if Defendant had a subjective expectation of privacy in the Dropbox account, it is not one that society is prepared to recognize as legitimate. It is true the jake.sawyer239@yahoo.com account was password protected, which may demonstrate a subjective expectation of privacy. It is also true however, that the password for the account was shared with multiple individuals. Defendant knew other individuals accessed the account. Defendant confirmed the Dropbox credentials with Dubois, adding "Now you have what I have." (*See* Doc. 12-1, PageID: 115). The fact that the account was password protected is irrelevant because access was granted to multiple individuals.

As discussed above, Dropbox provides a cloud based storage system for files. Those files are accessible so long as a user has a connection to Dropbox, the account information and the password. Courts have consistently held there is no reasonable expectation of privacy in files contained in peer-to-peer sharing services. *See United States v. Conner*, 521 Fed. App'x 493, 498 (6th Cir. Apr. 11, 2013); *United States v. Borowy*, 595 F.3d 1045, 1047-48 (9th Cir. 2010); *United States v. Stults*, 575 F.3d 834, 843 (8th Cir. 2009). Moreover, that determination is not changed simply when a defendant "closes" the network and grants access only to his "friends." *United States v. Sawyer*, 786 F. Supp. 2d 1352, 1356 (N.D. Ohio 2011) (no objectively reasonable expectation of privacy in files shared with a select group of "friends" via a file sharing software).

Accordingly, Defendant does not have an expectation of privacy in the jake.sawyer239@yahoo.com Dropbox account. He has not demonstrated a subjective expectation of privacy in the account. And even if he has, his expectation of privacy is not one

society is prepared to recognize as legitimate. Therefore, Defendant may not assert a Fourth Amendment challenge to the search of the Dropbox account.[3]

E. Suppression of Statements

Likewise, the Court will not suppress Defendant's statements to investigators because Defendant was not "in custody." "A defendant may not be 'compelled in any criminal case to be a witness against himself.'" *United States v. Swanson*, 341 F.3d 524, 528 (6th Cir. 2003) (quoting U.S. CONST. amend. V). "To the ends of protecting that right, *Miranda* [*v. Arizona*, 384 U.S. 436 (1966)] requires law-enforcement to give warnings, including the right to remain silent, before interrogating individuals whom the officers have placed 'in custody.'" *United States v. Panak*, 552 F.3d 462, 465 (6th Cir. 2009) (citing *Stansbury v. California*, 511 U.S. 318, 322 (1994)). To answer the "in custody" question, courts look to the "totality of the circumstances 'to determine how a reasonable man in the suspect's position would have understood the situation.'" *Swanson*, 341 F.3d at 528-29 (quoting *United States v. Salvo*, 133 F.3d 943, 948 (6th Cir. 1998)).

Several factors guide a court's inquiry into whether a defendant is in custody. Among those factors include: "the location of the interview; the length and manner of questioning; whether the individual possessed unrestrained freedom of movement during the interview; and whether the individual was told []he need not answer the question." *Panak*, 552 F.3d at 465. A

[3] In any event, Defendant's claim also fails on its merits. The Affidavit contains excerpts from the KIK conversations where the participants are actively exchanging and soliciting images of child pornography. Specific reference is made to the jake.sawyer239@yahoo.com account as an account where additional images are stored. Accordingly, the Affidavit provided the Magistrate Judge a substantial basis for concluding that probable cause existed to search the Dropbox account.

court analyzes these factors from the perspective of a reasonable person "innocent of any crime." *Id.* at 469 (quoting *United States v. Galloway*, 316 F.3d 624, 629 (6th Cir. 2003)).

After a review of the recorded interview with Defendant, the Court determines Defendant was not in custody. Upon entering the mobile lab, Agent Deterling explained the purpose of the search and showed Defendant a copy of the Search Warrant, which put everything in context for Defendant. Agent Deterling spoke in a clear, calm manner. He did not speak in an accusatory or aggressive tone. Agents did not restrain Defendant and Defendant was free to move throughout the interview. The fact that the questioning took place in a police vehicle is not dispositive to the analysis, since the location served as a private retreat away from other law-enforcement searching the Baintree residence. *See Oregon v. Mathiason*, 429 U.S. 492, 495-96 (questioning at the police office behind closed doors was not a custodial interrogation because defendant was informed he was not under arrest and was allowed to leave at the conclusion of the interview).

Most importantly, Agent Deterling informed Defendant he was not under arrest or in custody in any manner. *See Swanson*, 341 F.3d at 530 (collecting cases). Rather, Agent Deterling let Defendant know he could leave at any time Defendant desired. At that moment, a second agent opened the mobile lab's door to demonstrate it was unlocked. The agents told Defendant he could refuse to talk with them, return to the residence under supervision due to officer and his own safety or leave the premises entirely. Accordingly, the manner in which the agent conducted the initial part of the interview demonstrates that Defendant was free to leave the property and not answer questions. Despite this freedom, Defendant chose to remain with the agents and answer their questions.

Finally, the agents interviewed Defendant for one hour and twenty minutes. This amount

of time has repeatedly been held to be reasonable and not an indication that a Defendant is in custody. *See United States v. Mahan*, 190 F.3d 416, 422 (6th Cir. 1999) (an hour and half interview not demonstrative of custody).

While the Court does not discredit Defendant's claim that he felt some anguish when talking with investigators, the facts demonstrate Defendant was not forced to stay with the agents. *See Panack*, 552 F.3d at 471 ("The question in the end is not whether the individual felt pressure to *speak* to the officers but whether []he was forced to *stay* with them") (emphasis in original). Accordingly, when viewed from the perspective of a reasonable man innocent of any crime, Defendant was not in custody when he made certain statements and agents did not violate Defendant's Fifth Amendment rights.

F. Evidentiary Hearing

"An evidentiary hearing is required 'only if the motion is sufficiently definite, specific, detailed and non-conjectural to enable the court to conclude that *contested issues of fact* going to the validity of the search are in question.'" *United States v. Abboud*, 438 F.3d 554, 577 (6th Cir. 2006) (citations omitted) (emphasis supplied). A defendant must make some initial showing of contested facts to be entitled to such a hearing. *United States v. Giacalone*, 853 F.2d 470, 483 (6th Cir. 1988).

Defendant has not contested any material facts in the Affidavits. Rather, Defendant challenges the "four-corners" of the Affidavits, arguing that the Affidavits are legally insufficient to support a finding of probable cause. Because the Court previously determined otherwise, Defendant is not entitled to an evidentiary hearing on his Fourth Amendment challenges.

Furthermore, the Court's "in custody" analysis begins when agents brought Defendant into the mobile police lab. Authorities recorded the interview and the parties provided the recording to the Court for its consideration. After review of the recording, the Court determines that the facts undisputably demonstrate Defendant was not in custody at the time of the interview. Since there is no dispute of material fact, an evidentiary hearing on Defendant's Fifth Amendment claim is unnecessary.

III. CONCLUSION

Investigators conducted an above-board investigation into Defendant. They properly used administrative summonses to gather facts. The inclusion of the facts they found in the subsequent Affidavit for Search of Defendant's residence gave the Magistrate Judge a substantial basis to conclude probable cause existed to search the residence. Moreover, Defendant has not demonstrated a legitimate expectation of privacy in the Dropbox account. Furthermore, the totality of the circumstances demonstrate that Defendant was not in custody when he made inculpatory statements to agents. Accordingly, Defendant's Motion to Suppress (Doc. 10) is **DENIED**.

IT IS SO ORDERED.

s/ Christopher A. Boyko
CHRISTOPHER A. BOYKO
United States District Judge

Dated: June 4, 2019